ICFO

An efficient path to secure quantum keys

Renyi entropies, which are central to modern quantum key distribution security proofs, have traditionally been computationally difficult to optimize. ICFO researchers have now presented, in PRX Quantum article, a method to calculate them efficiently and reliably, yielding more stable security proofs.

September 14, 2026

It was 1984 when Bennett and Brassard designed the first quantum key distribution (QKD) protocol, BB84, and the field of quantum cryptography was born. More than 40 years later, researchers have successfully conducted numerous experiments, extended theoretical frameworks, and developed a plethora of novel QKD protocols. The fundamental idea, however, remains intact: Alice and Bob, two honest users who want to securely communicate, exchange and measure quantum states to obtain a secret key, solely relying on the laws of quantum physics to protect themselves against Eve, the smartest and most malicious eavesdropper.

To assess whether a QKD protocol is secure, it is essential to bound the amount of information Eve can actually gather from the interchanged quantum states. This has traditionally been computed through the so-called von Neumann entropy, but most modern security proofs now use the more general **Renyi entropy** instead, a family of entropies that accounts for how optimal or suboptimal the chosen measurements are. By introducing an additional optimization step over this set, researchers can get closer to the real key that Alice and Bob can achieve.

This optimization, however, is computationally difficult to solve. Current available approaches rely on ad hoc algorithms that are slow, numerically unstable, or applicable only to particular cases. That was the situation, at least, until **Mariana Navarro** and **Dr. Carlos Pascual Garcia**, researchers at ICFO who also work at Luxquanta (an ICFO spin-off that provides quantum cryptography solutions for companies and telecommunication networks), together with Andres Gonzalez Lorente, Pablo Parellada, and Dr. Mateus Araujo from the University of Valladolid, recently found a way to bypass these computational difficulties. By using well-established numerical methods (namely, conic optimization), the team has developed **a practical and reliable method to calculate Renyi entropies**.

? Reported in PRX Quantum, their conic optimization efficiently handles several QKD protocols, from the historical BB84 to the more demanding discrete-modulated continuous-variable QKD, which involves larger quantum systems and more complex experimental constraints.?

i¿½At first, we were amazed by the speed of our strategy,i¿½ recalls Mariana Navarro, irst author of the article. In the numerical benchmark for qubit BB84, for instance, the onic method solved the optimization in a fraction of a second, while comparable implementa ions took tens of seconds. i¿½Moreover, **our method is not only faster, but also more systematic and numerically precise than previous approaches**,i¿½ she add .

. The most natural next step would be to compute secure key rates for more compl x protocols, such as decoy-state BB84 and measurement-device-independent QKD. But according to Carlos Pascual Garcia, one of the senior researchers on the study, conic optimization also has the potential to unlock fairer comparisons of alternative protocol designs, accurately study channel loss or detector efficiency in an experiment, and provide practical insights into how far apart Alice and Bob can be while maintaining security.?

i¿½Forty years ago, not even Bennett and Brassard could have guessed how quan um cryptography would look today,i¿½ he reflects. i¿½The future is uncertain, and only ti e will tell the impact our study will have. But I am happy to share that we are already pursuin these broader goals, and preliminary results look really promisi

Reference:

Navarro, M., et. al., Finite-size quantum key distribution rates from Renyi entropies using conic optimization, PRX Quantum **7**, 033051 (2026).
DOI: https://doi.org/10.1103/bf9s-m4jb

Acknowledgements:
MN and CPG were supported by the Government of Spain (Severo Ochoa CEX2019-000910-S, FUNQIP and NextGeneration EU PRTR-C17.I1) and European Union (QSNP, 101114043). MN acknowledges funding from the European Union's Horizon Europe research and innovation programme under the MSCA Grant Agreement No. 101081441. CPG has received funding from the European Union's Digital Europe Programme under the project QUARTER (101091588) and Horizon 2020 Research and Innovation Programme under the project QSNP (101114043), and from the European Innovation Council's Horizon Europe EIC Accelerator Programme under the project MIQRO (101161539). The research of AGL, PVP, and MA was supported by the Q-CAYLE project, funded by the European Union-Next Generation UE/MICIU/Plan de Recuperacion, Transformacion y Resiliencia/Junta de Castilla y Leon (PRTRC17.11), and also by the Department of Education of the Junta de Castilla y Leon and FEDER Funds (Reference: CLU-2023-1-05). PVP has also been funded under the UVa 2024 predoctoral contract, co-financed by Banco Santander. MA was also supported by the Spanish Agencia Estatal de Investigacion, Grant Nos.~RYC2023-044074-I and PID2024-161725OA-I00.